UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION	MDL NO. 1:23-md-03083-ADB
This Document Relates To: DAWN ANN APPLEGATE, RICHARD APPLEGATE, and JON ROBUS, individually and on behalf of all others similarly situated, Plaintiffs, v. COREBRIDGE FINANCIAL, INC., AMERICAN GENERAL LIFE INSURANCE CO., PENSION BENEFIT INFORMATION, LLC, and PROGRESS SOFTWARE CORPORATION, Defendants.	**AMENDED CLASS ACTION COMPLAINT** CIVIL ACTION NO. 1:23-cv-12657

Plaintiffs Dawn Ann Applegate, Richard Applegate, and Jon Robus (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendants Corebridge Financial, Inc., its subsidiary American General Life Insurance Company ("American General") (collectively "Corebridge"), Pension Benefit Information, LLC ("PBI"), and Progress Software Corporation ("PSC") (together with Corebridge and PBI, "Defendants") based on personal knowledge with respect to themselves and upon information and belief derived from, among other things, investigation by their counsel and review of public documents, as to all other matters:

NATURE OF THE ACTION

1. Plaintiffs incorporate the allegations contained in Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

2. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated Corebridge customers' sensitive information, including names, Social Security numbers, policy/account number(s), dates of birth, and/or addresses ("personally identifiable information" or "PII").

3. As explained in detail herein, an unauthorized third party accessed Defendants' MOVEit Transfer servers and accessed and removed PII from the server as early as May 27, 2023 (the "Data Breach").

4. Corebridge is "one of the largest providers of retirement solutions and insurance products in the United States."[1]

5. Upon information and belief, current and former customers at Corebridge are required to entrust Defendants, directly or indirectly, with sensitive, non-public PII, without which Defendants could not perform their regular business activities, in order to obtain financial and/or other services. Defendants retain this information for many years and even after the consumer relationship has ended.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Before July 27, 2023, Corebridge learned that one of its vendors had been penetrated by a cyberattack and that "an unauthorized third party accessed one of our MOVEit Transfer servers on May 29, 2023, and May 30, 2023 and downloaded data."[2] The stolen data included the personal information of Plaintiffs and the Class Members.

[1] https://www.corebridgefinancial.com/who-we-are (last visited Aug. 29, 2023).
[2] The "Notice Letter". A sample copy is available at https://www.mass.gov/doc/assigned-data-breach-number-30124-nassau-life-and-annuity-company/download (last visited Aug. 30, 2023).

8. According to a letter sent to Plaintiffs and Class Members from PBI on behalf of Corebridge (the "Notice Letter"), the compromised PII included individuals' names, Social Security numbers, policy/account numbers, dates of birth, and address.[3]

9. Defendants failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

10. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants failure to: (i) adequately protect the PII of Plaintiffs and Class Members; and (ii) warn Plaintiffs and Class Members of its inadequate information security practices. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

11. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

12. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

[3] *Id.*

13. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

14. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

16. Plaintiffs also seek injunctive and equitable relief to prevent future injury on behalf of themselves and the putative Class.

PARTIES

17. Plaintiff Dawn Ann Applegate is, and at all times mentioned herein was, a citizen of Forked River, Ocean County, New Jersey.

18. Plaintiff Richard Applegate is, and at all times mentioned herein was, a citizen of Forked River, Ocean County, New Jersey.

19. Plaintiff Jon Robus is, and at all times mentioned herein was, a citizen of Crossville, Cumberland County, Tennessee.

20. Defendant Corebridge Financial, Inc. is a Delaware corporation with its principal place of business located at 2919 Allen Parkway, Woodson Tower #L4-01, Houston, Texas 77019. The registered agent for service of process is Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218.

21. Corebridge is a Vendor Contracting Entity of PBI. *See* Plaintiffs' Omnibus Set of Additional Pleading Facts, Appendix A.

22. Defendant American General Life Insurance Company is a Texas corporation, and wholly owned subsidiary of Defendant Corebridge Financial, Inc. with its principal place of business located at 2727-A Allen Parkway, Houston, Texas 77019. The registered agent for service of process is Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218.

23. PBI is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, MN 55402. PBI uses PSC's MOVEit service in the regular course of its business acting as a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans.[4]

24. PBI is a PSC Vendor. *See* Plaintiffs' Omnibus Set of Additional Pleading Facts, Appendix A.

25. PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

JURISDICTION AND VENUE

26. This action was originally filed in the United States District Court for the Southern District of Texas. This action was transferred to this Court for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407 and Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation.

27. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the

[4] https://www.pbinfo.com/ (last visited August 1, 2023).

State of Texas and have different citizenship from Defendants, including Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

28. The United States District Court for the Southern District of Texas has jurisdiction over Defendants because Defendants have sufficient contacts in Texas, as they conduct a significant amount of business in the state of Texas. Moreover, Corebridge has its principal place of business and headquarters in that District, and contracted with Plaintiff and the Class from that District.

29. United States District Court for the Southern District of Texas has jurisdiction over Corebridge because it operates in the Houston Division of the Southern District of Texas, and because it has its principal place of business and headquarters in the Houston Division of the Southern District of Texas.

30. Venue is proper in the United States District Court for the Southern District of Texas pursuant to 28 U.S.C. § 1391(a)(1) because Corebridge operates in that District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in that District, including Corebridge collecting and/or storing the PII of Plaintiff and Class Members.

FACTUAL ALLEGATIONS

Corebridge's Business

31. Corebridge is "one of the largest providers of retirement solutions and insurance products in the United States."[5]

32. Plaintiffs and Class Members are current and former customers of Corebridge.

33. As a condition of receiving its products and/or services, Corebridge requires that its customers, including Plaintiffs and Class Members, entrust it with highly sensitive personal information.

34. The information held by Corebridge in its and its vendor's computer systems at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

[5] https://www.corebridgefinancial.com/who-we-are (last visited Aug. 29, 2023).

35. Upon information and belief, Corebridge made promises and representations to its customers, including Plaintiffs and Class Members, that the PII collected from them as a condition of obtaining products and/or services at Corebridge would be kept safe, confidential, that the privacy of that information would be maintained, and that Corebridge would delete any sensitive information after it was no longer required to maintain it.

36. Indeed, Corebridge's Privacy Policy provides in relevant part:

> Corebridge Financial and its subsidiaries and affiliates ("we", or "us") are committed to protecting the privacy and Personal Information of the individuals we encounter in conducting our business… To protect your Personal Information, Corebridge Financial will take appropriate technical, physical, legal and organizational measures, which are consistent with applicable privacy and data security laws… When Corebridge Financial provides Personal Information to a service provider, the service provider will be selected carefully and required to use appropriate measures reasonably designed to protect the confidentiality and security of the Personal Information.[6]

37. Plaintiffs and Class Members provided their PII to Corebridge, directly or indirectly, with the reasonable expectation and on the mutual understanding that Corebridge would comply with its obligations to keep such information confidential and secure from unauthorized access.

38. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Corebridge to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

39. Corebridge had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its vendors and affiliates. Corebridge has a legal duty to keep consumer's PII safe and confidential.

[6] https://www.corebridgefinancial.com/privacy-policy (last visited Aug. 29, 2023).

40. Corebridge had obligations created by FTC Act, Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

41. Corebridge derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Corebridge could not perform the services it provides.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Corebridge assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

PBI's Business

43. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, and one of the many companies that uses PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[7]

44. According to the Notice Letter received by Plaintiff, PBI provides audit and address research services for Corebridge.

45. PBI's website also promises consumers that it has robust systems and processes in place to protect and secure their sensitive information:

[7] https://www.pbinfo.com/ (last visited August 1, 2023).

pbi

Protecting and securing the information of our clients and our company is of critical importance to PBI. We recognize that all relationships with current and prospective clients are based upon integrity and trust, and we take our role as custodians of confidential information very seriously.

PBI uses a multi-layered approach to protect data securely that includes, but is not limited to the following: implementing secure development practices, including annual training for our IT team, real time scanning of code changes for vulnerabilities, web application firewalls, n-tier application architecture, required security awareness training program for all employees at onboarding and on a regular basis, data loss prevention tools to alert and block transfers of sensitive data, and a consolidated SIEM solution that correlates alerts and events across multiple environments. PBI's data security team manages this multi-layered security architecture by performing over 30 security reviews of quarterly audit checks to test compliance against security policies.

PBI's formalized security program follows the industry-recognized security policy frameworks from the National Institute of Science & Technology (NIST) SP 800-53 and NIST Cybersecurity Framework.

SOC2 Audit and Third-party Security Testing

PBI undergoes an annual SSAE 18 SOC 2, Type II audit by an independent third-party to audit our controls over data confidentiality, integrity, security, and availability.

PBI regularly uses third parties to test and audit our security controls. We conduct monthly and quarterly vulnerability assessments and penetration tests of PBI's internal and external network and application security, and conduct annual application penetration tests.

46. PBI's website also tells consumers that it has systems and process in place to ensure the privacy of their sensitive information obtained over the internet and to prevent identity theft:

> **9. ONLINE PRIVACY**
>
> PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment.
>
> **10. IDENTITY THEFT**
>
> PBI strives to prevent the acquisition of information from our products and services for improper purposes, such as identity theft. PBI believes in the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual, as appropriate.

47. Furthermore, PBI acknowledges that it has a duty to safeguard Plaintiffs' and Class Members' sensitive PII and PHI because, *inter alia*, PBI's website tells consumers that it has systems in place to protect consumers' sensitive information, and routinely audits those systems to ensure they are compliant with federal regulations and other legislation—as well as industry standards and practices— governing data privacy:

> **8. ACCOUNTABILITY**
>
> PBI supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong privacy and information security protections are vital for an effective and trusted data industry.
>
> **11. COMPLIANCE**
>
> PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.

48. Discovery will show that through their provision of the foregoing services, PBI obtains possession of customers'—including Plaintiffs' and Class Members'—highly sensitive PII. Thus, in the regular course of their businesses, PBI collects and/or maintains the PII of consumers such as Plaintiffs and Class Members. PBI stores this information digitally in the regular course of business.

49. As evidenced by, *inter alia*, their receipt of the notice informing them that their PII were compromised in the Data Breach, Plaintiffs' and Class Members' PII was transferred using PSC's MOVEit service and/or they otherwise entrusted to Defendants their PII, from which Defendants profited.

50. Yet, contrary to PBI's website representations—by virtue of Defendants' admissions that they experienced the Data Breach—Defendants did not have adequate measures in place to protect and maintain sensitive PII and PHI entrusted to it. Instead, Defendants' websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII and PHI that is entrusted to them.

The Data Breach

51. On or about August 8, 2023, PBI, on behalf of Corebridge, began sending letters to Plaintiffs and other Data Breach victims (the "Notice Letter"), informing them that:

> **What happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that could be exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that an unauthorized third party accessed one of our MOVEit Transfer servers on May 29, 2023, and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review and have concluded that your personal information was involved in the incident. PBl has also notified law enforcement about this event.

> **What information was involved?** Our investigation determined that your personal information was impacted by this event and may have included: name, Social Security number, policy/account number, date of birth, and/or address.[8]

52. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

53. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

54. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendants failed to exercise due diligence in selecting its vendors and deciding with whom it would share sensitive PII.

55. The attacker accessed and acquired Defendants' files containing unencrypted PII of Plaintiffs and Class Members, including their Social Security numbers and other sensitive information.

56. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

57. Plaintiffs further believe their PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

Defendants Acquire, Collect, and Store Plaintiffs' and Class Members' PII

[8] Notice Letter.

58. As a condition to obtain products and/or services from Corebridge, Plaintiffs and Class Members were required to give their sensitive and confidential PII, directly or indirectly, to Corebridge.

59. Defendants retain and store this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiffs' and Class Members' PII, Defendants would be unable to perform their services.

60. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

61. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

62. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members or by exercising due diligence in selecting their vendors and properly auditing those vendors' security practices.

63. Upon information and belief, Corebridge made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

64. Indeed, Corebridge's Privacy Policy provides in relevant part:

> Corebridge Financial and its subsidiaries and affiliates ("we", or "us") are committed to protecting the privacy and Personal Information of the individuals we encounter in conducting our business… To protect your Personal Information, Corebridge Financial will take appropriate technical, physical, legal and organizational measures, which are consistent with applicable privacy and data security laws… When Corebridge Financial provides Personal Information to a service provider, the service provider will be selected carefully and required to use

appropriate measures reasonably designed to protect the confidentiality and security of the Personal Information.[9]

Defendants Knew or Should Have Known of the Risk Because Insurance Companies in Possession of PII Are Particularly Suspectable to Cyber Attacks

65. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting insurance companies that collect and store PII, like Corebridge, preceding the date of the Data Breach.

66. Data thieves regularly target companies like Defendants due to the highly sensitive information that they have custody of. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

67. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68 percent increase from 2020.[10]

68. Indeed, cyber-attacks, such as the one experienced by Corebridge, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

69. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

[9] https://www.corebridgefinancial.com/privacy-policy (last visited Aug. 29, 2023).
[10] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[11] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited Aug. 17, 2023).

records, May 2020), Corebridge knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

70. As a custodian of PII, Corebridge knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its or its vendor's data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

71. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

72. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if it or its vendor's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

73. Additionally, as companies became more dependent on computer systems to run their business,[12] *e.g.*, working remotely as a result of the COVID-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[13]

74. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on their server(s), amounting to potentially 798,000 individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

75. In the Notice Letter, PBI offers to cover identity monitoring services for a period of two years. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to

[12] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited Aug. 17, 2023).
[13] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited Aug. 17, 2023).

provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

76. PBI's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII was in fact affected, accessed, compromised, and exfiltrated from Defendants computer systems.

77. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

78. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

79. As an insurance company in possession of its current and former customers' PII, Corebridge knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its or its vendors' data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

80. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

[14] 17 C.F.R. § 248.201 (2013).

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

81. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[16]

82. For example, PII can be sold at a price ranging from $40 to $200.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

83. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names and Social Security numbers.

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[19]

85. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

---

[15] *Id*.
[16] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-howmuch-it-costs/ (last visited Aug. 17, 2023).
[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-informationis-selling-for-on-the-dark-web/ (last visited Aug. 17, 2023).
[18] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark/ (last visited Aug. 17, 2023).
[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 17, 2023).

86. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

Defendants Failed to Comply with FTC Guidelines

87. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

88. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Aug. 17, 2023).

89. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

90. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. These FTC enforcement actions include actions against insurance companies, like Corebridge.

92. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

93. Defendants were at all times fully aware of their obligation to protect the PII of its customers yet failed to comply with such obligations. Corebridge was also aware of the significant repercussions that would result from its failure to do so.

Corebridge Failed to Comply with the Gramm-Leach-Bliley Act

94. Corebridge is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

95. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

96. Corebridge collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Corebridge was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

97. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

98. Accordingly, Corebridge's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

99. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Corebridge violated the Privacy Rule and Regulation P.

100. Upon information and belief, Corebridge failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on its network systems as well as those of its vendors.

101. Corebridge failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

102. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

103. As alleged herein, Corebridge violated the Safeguards Rule.

104. Corebridge failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its vendors or verify the integrity of those systems.

105. Corebridge violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class Members with a non-affiliated third party without providing Plaintiffs

and Class Members: (a) an opt-out notice, and (b) a reasonable opportunity to opt out of such disclosure.

Defendants Failed to Comply with Industry Standards

106. As noted above, experts studying cybersecurity routinely identify insurance companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

107. Some industry best practices that should be implemented by insurance companies dealing with sensitive PII and their vendors, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and antimalware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

108. Other best cybersecurity practices that are standard in the insurance industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

109. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

110. Defendants failed to comply with these accepted standards in the insurance industry, thereby permitting the Data Breach to occur.

Defendants Breached their Duty to Safeguard Plaintiffs' and Class Members' PII

111. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols, and those of the parties with whom it shared PII, adequately protected the PII of Plaintiffs and Class Members.

112. Defendants breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
b. Failing to adequately protect Plaintiffs' and Class Members' PII;
c. Failing to properly monitor their data security systems for existing intrusions;
d. Failing to audit, monitor, or ensure the integrity their vendor's data security practices;
e. Failing to sufficiently train their employees and vendors regarding the proper handling of customers PII;
f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
g. Failing to adhere to the Gramm-Leach-Bliley Act and industry standards for cybersecurity as discussed above; and
h. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII.

113. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access their computer networks and systems which contained unsecured and unencrypted PII.

114. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

Common Injuries and Damages

115. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft

116. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

117. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

118. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

119. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

120. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

121. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[21]

[21] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited Aug. 17, 2023).

122. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

123. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

124. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft and Fraud

125. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

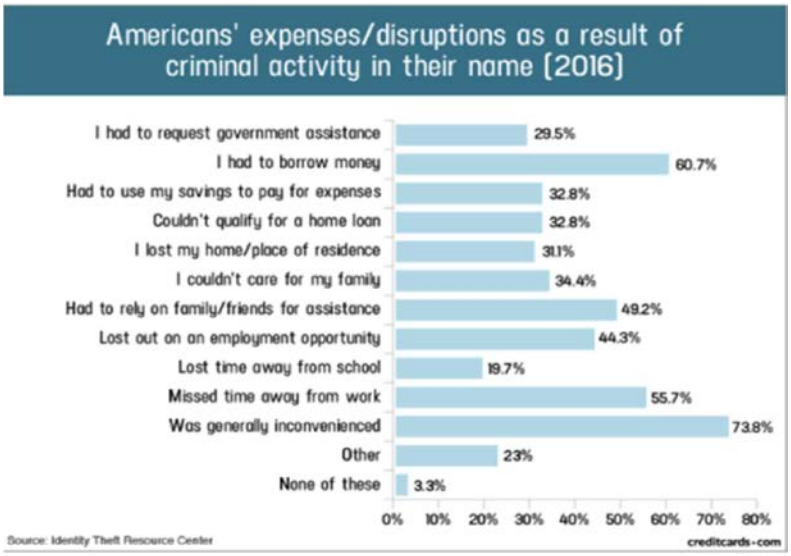
126. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as PBI's Notice Letter instructs, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

127. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

128. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[22]

129. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[23]

130. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[24]



[22] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[23] *See* Federal Trade Commission, *IdentityTheft.gov*, https://www.identitytheft.gov/Steps (last visited Aug. 17, 2023).

[24] *Credit Card and ID Theft Statistics*, Jason Steele (Oct. 24, 2017), available at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Aug. 17, 2023).

131. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

Diminution in Value of PII

132. PII is a valuable property right.[26] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

133. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[27]

134. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[28] [29]

135. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 per year.[30]

---

[25] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 17, 2023).

[26] *See, e.g.*, Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[27] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Aug. 17, 2023).

[28] https://datacoup.com/ (last visited Aug. 17, 2023).

[29] https://digi.me/what-is-digime/ (last visited Aug. 17, 2023).

[30] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Aug. 17, 2023).

136. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[31]

137. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available and the rarity of the data has been lost, thereby causing additional loss of value.

138. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, *e.g.*, names and Social Security numbers.

139. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

140. The fraudulent activity resulting from the Data Breach may not come to light for years.

141. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

142. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Corebridge's network, amounting to approximately 798,000

[31] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Aug. 17, 2023).

individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

143. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

144. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes–*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

145. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

146. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

147. The cost of credit monitoring and identity theft monitoring retails for around $200 per year per Class Member. This is a reasonable and necessary cost to monitor and protect Plaintiffs and Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendants' failure to safeguard their PII.

Plaintiff Dawn Ann Applegate's Experience

148. Plaintiff Dawn Ann Applegate has a life insurance policy with Corebridge, through its subsidiary United States Life Insurance Company. Ms. Applegate also at one time had a pension plan with American General.

149. As a condition of conducting business with Corebridge, Ms. Applegate was required to provide her PII, directly or indirectly, to Defendants, including her name, Social Security number, date of birth, and/or address.

150. At the time of the Data Breach—approximately May 29, 2023 through May 30, 2023— Defendants retained Ms. Applegate's PII in its system.

151. Ms. Applegate is very careful about sharing her sensitive PII. Ms. Applegate stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Ms. Applegate would not have entrusted her PII to Defendants had she known of their lax data security policies.

152. On or around August 25, 2023, Ms. Applegate received a Notice Letter in the mail dated August 8, 2023 from PBI on behalf of Corebridge. According to the Notice Letter, Ms. Applegate's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, policy/account number, date of birth, and/or address.

153. As a result of the Data Breach, and at the direction of Corebridge's Notice Letter, Ms. Applegate made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and checking her credit report and accounts for unauthorized activity. Ms. Applegate has spent significant time dealing with the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

154. Ms. Applegate suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and

certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

155. The Data Breach has caused Ms. Applegate to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

156. As a result of the Data Breach, Ms. Applegate anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

157. As a result of the Data Breach, Ms. Applegate is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

158. Ms. Applegate has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Richard Applegate's Experience

159. Plaintiff Richard Applegate has a life insurance policy with Corebridge, through its subsidiary United States Life Insurance Company. Mr. Applegate's wife also at one time had a pension plan with American General.

160. As a condition of conducting business with Corebridge, Plaintiff Richard Applegate was required to provide his PII, directly or indirectly, to Defendants, including his name, Social Security number, date of birth, and/or address.

161. At the time of the Data Breach—approximately May 29, 2023 through May 30, 2023— Defendants retained Mr. Applegate's PII in their system.

162. Mr. Applegate is very careful about sharing his sensitive PII. Mr. Applegate stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Mr.

Applegate would not have entrusted his PII to Defendants had he known of their lax data security policies.

163. On or around August 25, 2023, Mr. Applegate received a Notice Letter in the mail dated August 8, 2023 from PBI on behalf of Corebridge. According to the Notice Letter, Mr. Applegate's PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, policy/account number, date of birth, and/or address.

164. As a result of the Data Breach, and at the direction of Corebridge's Notice Letter, Mr. Applegate made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and checking his credit report and accounts for unauthorized activity. Mr. Applegate has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

165. Mr. Applegate suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

166. The Data Breach has caused Mr. Applegate to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

167. As a result of the Data Breach, Mr. Applegate anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

168. As a result of the Data Breach, Mr. Applegate is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

169. Mr. Applegate has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Jon Robus's Experience

170. As a condition of his workers' compensation structured settlement with Corebridge, Plaintiff Jon Robus was required to provide his PII, directly or indirectly, to Defendants, including his name, Social Security number, date of birth, and/or address.

171. At the time of the Data Breach—approximately May 29, 2023 through May 30, 2023— Defendants retained Mr. Robus's PII in their system.

172. Mr. Robus is very careful about sharing his sensitive PII. Mr. Robus stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Mr. Robus would not have entrusted his PII to Defendants had he known of its lax data security policies.

173. On or around August 25, 2023, Mr. Robus received a Notice Letter in the mail dated August 8, 2023 from PBI on behalf of Corebridge. According to the Notice Letter, Mr. Robus's PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, policy/account number, date of birth, and/or address.

174. As a result of the Data Breach, and at the direction of Corebridge's Notice Letter, Mr. Robus made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and checking his credit report and accounts for unauthorized activity. Mr. Robus has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

175. Mr. Robus suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value

of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

176. The Data Breach has caused Mr. Robus to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

177. As a result of the Data Breach, Mr. Robus anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

178. As a result of the Data Breach, Mr. Robus is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

179. Mr. Robus has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

180. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

181. Specifically, Plaintiff proposes the following classes (collectively, the "Class"), subject to amendment as appropriate:

(1) PSC Nationwide Class: All persons whose Personal Information was compromised in the MOVEit data breach.

(a) PSC New Jersey Class: All residents of New Jersey whose PII was compromised in the MOVEit data breach.

(b) PSC Tennessee Class: All residents of Tennessee whose PII was compromised in the MOVEit data breach

(2) PBI Nationwide Class: All persons whose PII was compromised on PBI's platform and/or systems in the MOVEit data breach.

(a) PBI New Jersey Class: All residents of New Jersey whose PII was compromised on PBI's platform and/or systems in the MOVEit data breach.

(b) PBI Tennessee Class: All residents of Tennessee whose PII was compromised on PBI's platform and/or systems in the MOVEit data breach.

(3) Corebridge Nationwide Class: All persons whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by Corebridge.

(a) Corebridge New Jersey Class: All residents of New Jersey whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by Corebridge.

(b) Corebridge Tennessee Class: All residents of Tennessee whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by Corebridge.

(4) American General Nationwide Class: All persons whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by American General.

(a) American General New Jersey Class: All residents of New Jersey whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by American General.

The foregoing state-specific classes are collectively referred to as the "State Classes" and the foregoing nationwide classes are collectively referred to as the "Nationwide Classes."

182. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any judge to whom this case is assigned as well as their judicial staff and immediate family members.

183. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

184. The proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

185. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of Class Members is unknown to Plaintiffs, upon information and belief approximately millions of individuals were impacted in the Data Beach. Thus, numerosity is met.

186. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;
b. Whether Defendants' conduct violated the FTCA and/or GBLA;
c. When Defendants learned of the Data Breach;
d. Whether Defendants' response to the Data Breach was adequate;
e. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' PII;
f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;
g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;
i. Whether Defendants owed a duty to Plaintiffs and Class Members to safeguard their PII;
j. Whether Defendants breached their duty to Plaintiffs and Class Members to safeguard their PII;

k. Whether hackers obtained Plaintiffs' and Class Members' PII via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

187. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

188. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

189. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

190. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Corebridge. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

191. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Corebridge has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

192. Finally, all members of the proposed Class are readily ascertainable. Corebridge has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Defendants.

COUNT 1
Negligence
On Behalf of Plaintiffs and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants

193. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

194. Corebridge requires its customers, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing its services.

195. Defendants gathered, stored, and shared the PII of Plaintiffs and Class Members as part of their business of soliciting its services to its customers, which solicitations and services affect commerce.

196. Plaintiffs and Class Members entrusted Defendants with their PII, directly or indirectly, with the understanding that Defendants would safeguard their information.

197. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

198. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to exercise due diligence in selecting vendors and to audit, monitor, and ensure the integrity of their data systems and practices and to give prompt notice to those affected in the case of a data breach.

199. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

200. Defendants' duty to use reasonable security measures also arose under the GLBA, under which it was required to protect the security, confidentiality, and integrity of customer

information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

201. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its and its vendor's systems and networks, and the personnel responsible for them, adequately protected the PII.

202. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of being customers of Corebridge.

203. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Corebridge is bound by industry standards to protect confidential PII.

204. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

205. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

206. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

207. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Class in their possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was and is necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

208. Defendants breached their duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect

Plaintiffs' and Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of their data security practices;

d. Allowing unauthorized access to Plaintiffs' and Class Members' PII;

e. Failing to detect in a timely manner that Plaintiffs' and Class Members' PII had been compromised;

f. Failing to remove former customers' PII they were no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Plaintiffs and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

209. Defendants violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

210. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

211. Defendants violation of Section 5 of the FTC Act and GLBA constitutes negligence.

212. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

213. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

214. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs' and Class Members' PII would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

215. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

216. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on their systems.

217. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII would result in one or more types of injuries to Plaintiffs and Class Members.

218. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

219. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

220. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

221. Defendants have admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

222. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

223. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

224. Defendants' conduct, as alleged herein, allowed it to gain a competitive advantage over companies offering the same or similar services because, rather than properly implement data security protocols, or verify the integrity of its vendor's systems, as required by statute and industry standards, Corebridge diverted money intended to apply to data security towards its own profit. Defendants' conduct, and the unfair advantage realized thereby, creates a race to the bottom by encouraging companies to divert funds intended for data security towards profits in order to remain competitive. The end effect is that both consumers and the marketplace in general are harmed through the widespread adoption of substandard data security practices and the concomitantly increased risk of cyberattacks and fraud and identity theft (which disrupt the lives of victims and impose a burden on the state to investigate and prevent criminal activity).

225. By collecting and taking custody of Plaintiffs' and Class Members' PII with full awareness of both the likelihood of a cyberattack targeted to acquire that information and the severe consequences that would result to Plaintiffs and Class Members if the confidentiality of the PII was breached, Defendants assumed a special relationship that required it to guard against the foreseeable conduct of a criminal third party. If Defendants had not intervened by taking charge of Plaintiffs' and Class Member's PII, no harm would have resulted to Plaintiffs and Class Members as a result of the Data Breach.

226. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

227. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

228. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

229. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

230. Defendants' negligent conduct is ongoing, in that they still hold the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

231. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT 2

Breach of Implied Contract
On Behalf of Plaintiffs and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants

232. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

233. Plaintiffs and Class Members were required to provide their PII to Defendants as a condition of receiving insurance, financial, and/or other services from Corebridge.

234. Plaintiffs and the Class entrusted their PII to Defendants. In so doing, Plaintiffs and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

235. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants data security practices complied with relevant laws and regulations and were consistent with industry standards.

236. Implicit in the agreement between Plaintiffs and Class Members and Defendants to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

237. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Corebridge, on the other, is demonstrated by their conduct and course of dealing.

238. Corebridge solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their PII to Defendants.

239. In accepting the PII of Plaintiffs and Class Members, Defendants understood and agreed that they were required to reasonably safeguard the PII from unauthorized access or disclosure.

240. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiffs and Class Members that they would only disclose PII under certain circumstances, none of which relate to the Data Breach.

241. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

242. Plaintiffs and Class Members paid money and provided their PII to Defendants with the reasonable belief and expectation that Defendants would use part of their earnings to obtain adequate data security. Defendants failed to do so.

243. Plaintiffs and Class Members would not have entrusted their PII to Corebridge in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

244. Plaintiffs and Class Members would not have entrusted their PII to Corebridge in the absence of its implied promise to monitor its and its vendor's computer systems and networks to ensure that it adopted reasonable data security measures.

245. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

246. Defendants breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

247. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

248. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

249. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT 3
Unjust Enrichment
On Behalf of Plaintiffs and the Nationwide Classes, and the State Classes in the Alternative, Against All Defendants

250. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

251. This count is pleaded in the alternative to the Breach of Implied Contract claim above (Count 2).

252. Plaintiffs and Class Members conferred a monetary benefit on Defendants.

253. Specifically, they paid for services from Corebridge and/or its agents and in so doing also provided Defendants with their PII. In exchange, Plaintiffs and Class Members should have received from Defendants the services that were the subject of the transaction and should have had their PII protected with adequate data security.

254. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendants profited from Plaintiffs' and Class Members' retained data and used Plaintiffs' and Class Members' PII for business purposes.

255. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

256. Defendants acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

257. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have entrusted their PII with Defendants or obtained services at Corebridge.

258. Plaintiffs and Class Members have no adequate remedy at law.

259. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon them.

260. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

261. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

262. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendants to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. Prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its and its vendor's systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of its network is compromised, hackers cannot gain access to other portions of its systems;

x. Requiring Defendants to conduct regular database scanning and securing checks;

xi. Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. Requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendants to implement a system of tests to assess their employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with its policies, programs, and systems for protecting PII;

xiv. Requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor its information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from its servers; and

xvii. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. Ordering Defendants to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

DATED: June 12, 2024

Respectfully Submitted,

/s/ Kristen A. Johnson
Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

Joe Kendall
Texas State Bar No. 11260700
SDTX Bar No. 30973
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, TX 75219
Telephone: 214-744-3000
Facsimile: 214-744-3015
jkendall@kendalllawgroup.com

Timothy W. Emery*
Patrick B. Reddy*
Paul Cipriani*
EMERY REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
Phone: (206) 442-9106
Fax: (206) 441-9711
Email: emeryt@emeryreddy.com
Email: reddyp@emeryreddy.com
Email: paul@emeryreddy.com

M. Anderson Berry*
Gregory Haroutunian*
CLAYEO C. ARNOLD, A PROFESSIONAL CORP.

865 Howe Avenue
Sacramento, CA 95825
Phone: (916) 239-4778
Fax: (916) 924-1829
Email: aberry@justice4you.com
gharoutunian@gmail.com

*admitted *pro hac vice*

Attorneys for Plaintiffs and the Proposed Class

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 12, 2024

/s/ Kristen Johnson
Kristen Johnson